Claims

1) A method comprising:

exchanging data between a SIM device and an application executed in a trusted platform, wherein the data to be exchanged is secured from unauthorized access.

2) The method of claim 1, wherein the exchanging of data include:

exchanging an encryption key via a trusted path within a computer system; and

exchanging data encrypted with the encryption key, via an untrusted path within the computer system.

3) The method of claim 2, wherein the exchanging the encryption key includes the application transmitting the encryption key to a protected section of memory within the computer system; and

a SIM device accessing the encryption key from the protected section of memory.

4) The method of claim 2, wherein the exchanging the encryption key includes the application accessing the encryption key from the SIM device, the application accessing the encryption key via a trusted port of a chipset.

5) The method of claim 2, wherein the exchanging the encryption key includes exchanging multiple encryption keys, and the exchanging data includes exchanging separate units of data, with each unit of data separately encrypted with an encryption key selected from the multiple encryption keys.

6) The method of claim 2, wherein the exchanging data includes a host controller transmitting data from the SIM device to an unprotected section of memory.

7) The method of claim 6, wherein the exchanging data includes a driver transmitting data from the unprotected section of memory to the application.

8) The method of claim 7, wherein the host controller is a Universal Serial Bus (USB) host controller and the driver is a USB driver.

9) The method of claim 6, wherein the exchanging the encryption key includes the SIM device reading the encryption key from the protected section of memory via a trusted port of a chip set.

10) The method of claim 6 further including:

the application decrypting the encrypted data using the encryption key.

11) The method of claim 7 further including

prior to exchanging the encryption key, the application authenticating the SIM device.

12) The method of claim 6, further including:

exchanging a new encryption key based on a predetermined event selected from a group comprising of, each new transaction, passage of a predetermined period of time, and exchange of a predetermined amount of data.

13) A system comprising:

a processor;

a memory having a protected section and an unprotected section;

a SIM device; and

a chipset to Exchange data between the SIM device and an application executed in a trusted platform, wherein the data to be exchanged is secured from unauthorized access.

14) The system of claim 11, wherein the exchange of data is to include an exchange of an encryption key via a trusted path within a computer system, and an exchange of data encrypted with the encryption key, via an untrusted path within the computer system.

13) The system of claim 12, wherein the exchange of the encryption key includes the application to transmit the encryption key to the protected section of memory, and the SIM device to access the encryption key from the protected section of memory.

14) The system of claim 14, wherein the exchange of the encryption key includes the application to access the encryption key from the SIM device, the application to access the encryption key via a trusted port of a chipset.

15) The system of claim 14, wherein the exchange of the encryption key includes an exchange of multiple encryption keys, and the exchange of data includes an exchange of separate units of data, with each unit of data separately encrypted with an encryption key selected from the multiple encryption keys.

14) The system of claim 12, wherein the system further includes a host controller to transmit data from the SIM device to an unprotected section of memory.

15) The system of claim 14, wherein the system further includes a driver to transmit data from the unprotected section of memory to the application.

16) The system of claim 15, wherein the host controller is a Universal Serial Bus (USB) host controller and the driver is a USB driver.

17) The system of claim 14, wherein the SIM device is to read the encryption key from the protected section of memory via a trusted port of the chip set.

18) The system of claim 14, wherein the application is to decrypt the encrypted data using the encryption key.

19) The system of claim 15, wherein the application is to authenticate the SIM device prior to the exchange of the encryption key.

20) The system of claim 14, wherein a new encryption key is to be exchanged based on a predetermined event selected from a group comprising of, each new transaction, passage of a predetermined period of time, and exchange of a predetermined amount of data.